REMARKS

This application has been carefully reviewed in light of the Office Action dated May 4, 2004. Claims 1 to 3, 6, 7, 10 to 14, 18 to 20 and 22 to 28 are pending in the application, of which Claims 1, 10, 14, 18, 20 and 22 are independent. Reconsideration and further examination are respectfully requested.

In the Office Action, all claims were rejected under 35 U.S.C. § 103(a), with Claims 1, 3, 6 and 10 to 14 having been rejected over U.S. Patent No. 5,619,025 (Hickman) in view of U.S. Patent No. 6,192,473 (Ryan), Claims 2 and 11 having been rejected over Hickman in view of Ryan and further in view of Official Notice taken by the Examiner, Claims 7, 18 to 20 and 22 having been rejected over Hickman in view of Ryan and further in view of Schneier (Applied Cryptography), Claims 1, 6, 10, 13 and 14 having been rejected over U.S. Patent No. 5,534,857 (Laing) in view of U.S. Patent No. 6,192,473 (Ryan), Claims 2, 3, 11 and 12 having been rejected over Laing in view of Ryan and further in view of Official Notice taken by the Examiner, and Claims 7, 18 to 20 and 22 having been rejected over Laing in view of Ryan and further in view of Schneier (Applied Cryptography). Reconsideration and withdrawal of the rejections are respectfully requested.

The present invention concerns an image input apparatus. According to one aspect of the invention, the apparatus reads an encryption key stored in an external source (such as an Integrated Circuit (IC) card connected to the apparatus) and stores the card internally. The apparatus then uses the stored encryption key to encrypt digital information (such as an image scanned in by a scanner of the apparatus). Once the encryption has been completed, the stored encryption key is erased from the apparatus and the encrypted digital information is output. Thus, since the encryption key is read from the external source, is

only temporarily stored in the apparatus and is promptly erased upon completion of the encryption, it is less likely that a hacker can obtain the encryption key from the apparatus. Moreover, since the key is controlled by, and is only known to the holder of the external source in which the key is stored, it is less likely that the key can be obtained by an unauthorized user.

Another feature of the image input apparatus is the ability to receive and decrypt the encrypted digital information. According to this aspect, when the foregoing encrypted digital information is output for example, by one of multiple image input apparatuses that include the claimed features, the encrypted data can be received by the image output apparatus. However, in order to decrypt and process the data, a decryption key corresponding to the encryption key used to encrypt the information must be obtained. For example, the holder of the IC card that stores the encryption key connects the IC card to the apparatus so that the decryption key can be obtained. The apparatus then decrypts the digital information using the obtained decryption key so that the information can be processed. Thus, with the present invention, the image output apparatus can perform both the encryption and outputting of digital information using the unique key stored in the external source, and can also obtain the unique key from the external source and decrypt received information.

Referring specifically to the claims, amended independent Claim 1 is an image input apparatus comprising reading means for reading an encryption key stored in an external source, storage means for storing the read encryption key to execute an encryption process, encryption means for encrypting digital information with the encryption key stored in the storage means, output means for outputting the encrypted digital information, erasing means for erasing the encryption key stored in the storage means after encrypting the

digital information by the encryption means, input means for inputting digital information encrypted with the encryption key stored in the external source, obtaining means for obtaining, from the external source, a decryption key corresponding to the encryption key, and decryption means for decrypting the input encrypted digital information by using the decryption key obtained by the obtaining means.

Amended independent Claims 10 and 14 are method and computer-readable medium claims, respectively, that substantially correspond to Claim 1.

Amended independent Claim 18 includes features along the lines of Claim 1, but is more specifically directed to an image input apparatus comprising generating means for generating an internal key, information encryption means for encrypting digital information with the internal key, reading means for reading an external encryption key stored in an external source, storage means for storing the external encryption key to execute a key encryption process, key encryption means for encrypting the internal key with the external encryption key stored in the storage means, output means for outputting the encrypted digital information and the encrypted internal key, erasing means for erasing the external encryption key and the internal key after executing the encryption process by the information encryption means and the key encryption means, input means for inputting encrypted digital information and an encrypted internal key, obtaining means for obtaining an external decryption key corresponding to the external encryption key stored in the external source, key decryption means for decrypting the input encrypted internal key with the obtained external decryption key, and decryption means for decrypting the input encrypted digital information with the internal key decrypted by the key decryption means.

Amended independent Claims 20 and 22 are method and computer-readable medium claims, respectively, that substantially correspond to Claim 18.

The applied art, alone or in any permissible combination, is not seen to disclose or to suggest the features of the present invention. More particularly, with respect to Claims 1, 10 and 14, the applied art is not seen to disclose or to suggest at least the feature of an image input apparatus that encrypts digital information with an encryption key read from an external source and stored in a storage means of the apparatus, erases the stored encryption key after encrypting the digital information, inputs digital information encrypted with the encryption key stored in the external source, obtains, from the external source, a decryption key corresponding to the encryption key, and decrypts the input encrypted digital information by using the obtained decryption key. Similarly, with respect to Claims 18, 20 and 22, the applied art is not seen to disclose or to suggest at least the feature of an image input apparatus encrypting an internally generated key, used to encrypt digital information, with an external encryption key read from and external source and stored in a storage means of the image input apparatus, erasing the external encryption key and the internal key after executing the encryption process, obtaining an external decryption key corresponding to the external encryption key stored in the external source, decrypting the encrypted internal key, input with encrypted digital information, with the obtained external decryption key, and decrypting the input encrypted digital information with the decrypted internal key.

Hickman is merely seen to disclose a laser and crystal diode technique for verifying a document such as a credit card. Hickman discloses that the image data (the refractive characteristics of the crystals used on a magnetic stripe of a credit card) may be used as an encryption key and the encryption key may be used to transmit data to an electronic database. Additionally, Hickman specifically states that "[a]fter a transmission is completed, the encryption key is erased immediately in the database bank, thus insuring

internal security of data transmission." However, Applicant fails to see anything in Hickman in which a decryption key is stored in the credit card such that it can be obtained and used to decrypt received data that has been encrypted with the encryption key. Accordingly, Hickman is not seen to disclose or to suggest the features of the present invention.

Ryan is merely seen to disclose that, after performing a requested function, an unencrypted form of a K_{KMS} key is erased, with an encrypted form of the K_{KMS} key being maintained in a database. However, only the unencrypted form of the key is erased and the encrypted form of the key is maintained in the database. Moreover, Ryan is not seen to disclose anything with regard to the apparatus inputting digital information encrypted with the encryption key stored in the external source, obtaining, from the external source, a decryption key corresponding to the encryption key, and decrypting the input encrypted digital information by using the obtained decryption key. Therefore, Applicant believes that any permissible combination of Hickman and Ryan would not have resulted in the presently claimed invention.

Referring to paragraph 5 at page 2 of the Office Action (under Response to Arguments), the Examiner asserts that, with regard to Applicant's previous assessment of Ryan, "[p]art of applicant's confusion might stem from the author of Ryan, Jr. et al.'s horribly misrepresenting the system". The Office Action then he proceeds to apply the Examiner's own interpretation of what he believes Ryan should disclose. This position is fatally flawed since it is simply impermissible for the Examiner to interject his own disclosure into a reference so as to assert what is thought should be disclosed in the reference, rather than simply taking the actual disclosure of Ryan at face value and applying it to the claims. If the author of Ryan horribly misrepresented its system as the

Office Action asserts, then unfortunately for the patent Examiner, he is simply stuck with that horrible misrepresentation as the teaching of Ryan. Thus, Applicant submits that the alleged disclosure of Ryan, as asserted in the Office Action, is erroneous and should be withdrawn.

Laing is merely seen to disclose a system for securely writing information onto a smart card so that user secret codes can be stored on the smart card. The smart card includes a cipher key that is merely used as part of a validation process to validate the smart card. However, Laing is not seen to disclose or to suggest at least the feature of an image input apparatus that encrypts digital information with an encryption key read from an external source and stored in a storage means of the apparatus, erases the stored encryption key after encrypting the digital information, inputs digital information encrypted with the encryption key stored in the external source, obtains, from the external source, a decryption key corresponding to the encryption key, and decrypts the input encrypted digital information by using the obtained decryption key (Claims 1, 10 and 14), or at least the feature of an image input apparatus encrypting an internally generated key, used to encrypt digital information, with an external encryption key read from and external source and stored in a storage means of the image input apparatus, erasing the external encryption key and the internal key after executing the encryption process, obtaining an external decryption key corresponding to the external encryption key stored in the external source, decrypting the encrypted internal key, input with encrypted digital information, with the obtained external decryption key, and decrypting the input encrypted digital information with the decrypted internal key (Claims 18, 20 and 22).

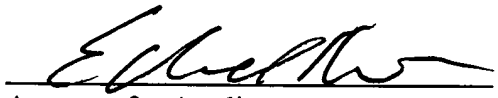
Schneier is not seen to add anything to overcome the deficiencies of Hickman, Ryan and Laing, and is also not seen to disclose or to suggest at least the feature of an image input apparatus that encrypts digital information with an encryption key read from an external source and stored in a storage means of the apparatus, erases the stored encryption key after encrypting the digital information, inputs digital information encrypted with the encryption key stored in the external source, obtains, from the external source, a decryption key corresponding to the encryption key, and decrypts the input encrypted digital information by using the obtained decryption key (Claims 1, 10 and 14), or at least the feature of an image input apparatus encrypting an internally generated key, used to encrypt digital information, with an external encryption key read from and external source and stored in a storage means of the image input apparatus, erasing the external encryption key and the internal key after executing the encryption process, obtaining an external decryption key corresponding to the external encryption key stored in the external source, decrypting the encrypted internal key, input with encrypted digital information, with the obtained external decryption key, and decrypting the input encrypted digital information with the decrypted internal key (Claims 18, 20 and 22).

In view of the foregoing, any permissible combination of Hickman, Ryan, Laing and/or Schneier, is not believed to disclose or to suggest the features of the present invention. Accordingly, all of amended independent Claims 1, 10, 14, 18, 20 and 22, as well as the claims dependent therefrom, are believed to be in condition for allowance.

No other matters having been raised, the entire application is believed to be in condition for allowance and such action is respectfully requested at the Examiner's earliest convenience.

Applicant's undersigned attorney may be reached in our Costa Mesa, California office at (714) 540-8700. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,



Attorney for Applicant
Edward A. Kmett
Registration No. 42,746

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-2200
Facsimile: (212) 218-2200

CA_MAIN 83947v1